REMARKS

2-3. 35 U.S.C. § 112. Rejections.

Claims 1-15 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to point out and distinctly claim the subject matter which applicant regards as the invention.

The Office Action states that "In Claim 1, line 16, there is no proper antecedent basis for "said remote location"."

Applicant has amended Claim 1, to replace "remote" with –redemption--, to provide proper antecedent basis for the claimed structure.

The Office Action also states that "In Claim 1, it is not clear as to what is meant by "to a holder".

Applicant has amended independent Claim 1 and independent Claim 16, to claim that the holder is comprises "any of said acquirer user and an alternate recipient of said issued certificate to whom said acquirer user has communicated said private key".

Support is seen in the Application as filed, at least on page 7, lines 18-23; on page 10, lines 6-10; on page 14, lines 8-11; on page 23, lines 8-16; on page 24, lines 1-11; on page 27, lines 1-4; and in Figure 4 (ACQ,RCP) .

Applicant has also amended dependent Claim 10 and dependent Claim 25, to provide proper antecedent basis for the "alternate recipient", as claimed in independent Claim 1 and independent Claim 16, respectively.

Applicant therefore respectfully submits that Claim 1, as amended, overcomes the rejections under 35 U.S.C. §112, second paragraph. As Claims 2-15 depend from amended independent Claim 1, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

4-6. 35 U.S.C. § 103. Rejections.

5. Claims 1-11, 13-26 and 28-30 are rejected under 35 U.S.C. §103(a) as being unpatentable over Franklin et al (U.S. Patent No. 6,000,832) in view of Lee et al (U.S. Patent No. 6,170,744 B1).

Regarding Claims 1, 9, 15, 16, 24 and 30, the Office Action states that "Franklin et al teach an electronic online commerce card such that Applicant's certificate authority reads on element 32 and column 9, lines 4-11, Applicant's virtual certificate reads on the electronic online commerce card, Applicant's redemption denomination reads on the customer's credit/debit limit, Applicant's first public key identifier reads on the inherent public key which would correspond to the assigned private key, column 2, lines 17-19 and column 8, lines 21-24, Applicant's certificate issuance module reads on the software module used to formulate transaction numbers, Applicant's certificate including redemption denomination and first public key identifier reads on the customer's credit card/debit card and column 8, lines 21-24 respectively, Applicant's storing of redemption denomination, first public key identifier and private key reads on the customer database, element 62, Applicant's authenticating module reads on the issuing institution and column 2, lines 51-55, and Applicant's canceling means reads on the inherent rejection of the authorization request if the customer data in the request is not correct."

The Office Action also states that "while Franklin et al do not teach that their certificate can be used for off-line transactions, Lee et al teach a system for self-authenticating negotiable documents wherein a check (certificate) is printed for use to pay anything that would normally be paid by a check; this inherently includes off-line, in store, payments of transactions. Lee et al also teach that their check includes a bar code, element 110, containing information similar to the information contained in Franklin's virtual certificate, such as amount of check (redemption denomination), hash code, public key and account number. Therefore, it is considered that it would have been obvious to one of ordinary skill in the art at the time of the invention to utilize the teachings of Lee et al in the system of Franklin et al so that a physical form of a certificate can be used in off-line transactions."

Applicant has amended independent Claim 1, to claim a certificate system on a network, comprising:

a certificate authority connected to said network, said certificate authority adapted to allow the definition of a virtual certificate comprising a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

a certificate issuance module for creation of an issued certificate upon selectable acquisition of said virtual certificate by an acquirer user across said network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation of said issued certificate associated with a private key which is assigned at time of said acquisition of said virtual certificate, wherein said private key does not appear on said issued certificate, and wherein said redemption denomination, said first public key identifier, and said assigned private key are stored at said certificate authority in association with said issued certificate;

a certificate authentication module for authorization of an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate located at said redemption location, said holder comprising any of said acquirer user and an alternate recipient of said issued certificate to whom said acquirer user has communicated said private key, said authorization based upon a communication from said redemption location to said certificate authority of said redemption denomination and said first public key identifier from said issued certificate, a communication of said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

means to cancel further redemption of said issued certificate at said certificate authority.

Applicant has also amended independent Claim 16, to claim a process within a transaction network, comprising the steps of:

defining a virtual certificate on a certificate authority, said defined virtual certificate comprised of a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

creating an issued certificate upon acquisition of said virtual certificate by an acquirer user on said transaction network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation of said issued certificate associated with an establishment of a private key which does not appear on said issued certificate, said redemption denomination, said first public key identifier, and said established private key stored at said certificate authority in association with said issued certificate;

authorizing an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate, said holder comprising any of said acquirer user and an alternate recipient of said issued certificate to whom said acquirer user has communicated said private key, wherein said authorization is based upon redemption submittal at said redemption location of said redemption denomination and said first public key identifier from said issued certificate, a communication of said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

canceling further redemption of said issued certificate at said certificate authority.

Support is seen in the Application as filed, as least on page 7, lines 6-26; on page 9, line 10 to page 10, line 12; on page 11, lines 1-23; on page 13, line 6 to page 14, line 29; on page 23, lines 8-16; on page 26, line 20 to page 27, line 29; in Figure 1 to Figure 4, and in Figure 8. Details regarding issued, *i.e.* acquired certificates are seen in the Application as filed, at least on page 22, line 31 to page 24, line 11; in Figure 2; in Figure 3; and in Figure 4.

As seen above, Applicant has amended independent Claim 1 and independent Claim 16, to claim that the creation of the issued certificate is associated with a private key which is assigned at time of said acquisition of said virtual certificate,

wherein the private key does not appear on said issued certificate. Support is seen on page 14, lines 1-4, wherein:

> "The established private key 76 does not appear on the certificate 60, and is known only to the acquirer user ACQ, but is stored by the certificate authority 12, in association with the other data elements relating to the certificate 60, on the secure database 18."

Further support for the private key which is associated with an issued certificate is seen in the Application as filed, at least on page 13, lines 6-31; on page 22, lines 2-20; and on page 24, lines 24-26.

As well, as seen in independent Claim 1 and independent Claim 16, as amended, authorization of the redemption of an issued certificate requires a communication of the private key provided by the holder, and a matching comparison of the redemption denomination, the first public key identifier, and the private key stored at said certificate authority. Support is seen in the Application as filed, at least on page 7, lines 20-26; on page 10, lines 6-12; on page 14, line 6 to page 15, line 16; on page 27, lines 1-23; on page 27, line 31 to page 28, line 3; and in Figure 2, Figure 3, and Figure 4.

The advantageous use of a private key which does not appear on an issued certificate is seen in the Application as filed, at least in Figure 4, in Figure 6, and on page 24, lines 13-26, wherein:

> "As seen in Figure 6, until an acquired certificate is redeemed, an acquirer preferably has the ability to cancel 152 a previously acquired certificate 60, or to request that an acquired certificate be revoked and replaced 153 by a new certificate 60. For example, if an acquirer user accidentally damages, destroys, or loses a previously printed acquired certificate 60, the acquirer may simply print out a new certificate 60, or

have a new certificate delivered or faxed, and may either retain the previously stored private key 76, or may specify a new private key 76.

Since an acquired certificate 60 may only be used for redemption once (at which time further use is revoked), there is no financial risk to the issuer ISR in the use of replacement certificates 60, or that a downloaded certificate 60 be printed more than once. As well, even if a certificate is lost and retrieved by a second party, or is stolen, the lost acquired certificate is unredeemable, without submittal of the private key 76, which is not included as printed information on a certificate 60."

While Franklin et al describe an electronic online commerce card with customer generated transaction proxy number for online transactions, Applicant respectfully submits that the online commerce card described by Franklin is significantly different than the present invention, as claimed in Claim 1 and Claim 16, as amended. An overview of the electronic online commerce card, as disclosed by Franklin et al, is seen at least in the Abstract, wherein:

"An online commerce system facilitates online commerce over a public network using an online commerce card. The "card" does not exist in physical form, but instead exists in digital form. It is assigned a customer account number that includes digits for a prefix number for bank-handling information, digits for a customer identification number, digits reserved for an embedded code number, and a digit for check sum. The bank also gives the customer a private key. During an online transaction, the customer computer retrieves the private key and customer account number from storage. The customer computer generates a code number as a function of the private key, customer-specific data (e.g., card-holder's name, account number, etc.) and transaction-specific data (e.g., transaction amount, merchant ID, goods ID, time, transaction date, etc.). The customer computer embeds the code number in the reserved digits of the customer account number to create a transaction number specific to the transaction. The customer submits that transaction number to the merchant as a proxy for a regular card number. When the merchant

submits the number for approval, the issuing institution recognizes it as a proxy transaction number, indexes the customer account record, and looks up the associated private key and customer-specific data. The institution computes a test code number using the same function and input parameters as the customer computer. The issuing institution compares the test code number with the code number embedded in the transaction number. If the two numbers match, the issuing institution accepts the transaction number as valid."

Applicant respectfully submits that while Franklin et al describe an online commerce card for online transactions, Franklin et al do not disclose or suggest the creation of an issued certificate that is associated with an establishment of a private key which does not appear on the issued certificate, nor does Franklin et al disclose or suggest an authorization which is based upon a submittal at the redemption location of the redemption denomination and the first public key identifier from the issued certificate, a communication of the private key provided by the holder, and a matching comparison of the redemption denomination, the first public key identifier, and the private key stored at said certificate authority.

Furthermore, while Lee et al describe a self-authenticating negotiable document, Applicant respectfully submits that the self-authenticating negotiable document described by Lee et al is significantly different than the present invention, as claimed in Claim 1 and Claim 16, as amended. An overview of the self-authenticating negotiable document, as disclosed by Lee et al, is seen at least in the Abstract, wherein:

"A self-authenticating document is created by providing a one-way hash value in a symbol creation process, and then using a public key to decrypt data of the self-authenticating document. Raw data to be provided with the self-authenticating document is received, and an account digital signature key is retrieved and used to sign the raw data. A non-repudiation hash value from a previously-created self-authenticating document is utilized, and the raw data and the digital signature key is combined with the hash value to create a new hash value for the self-

authenticating document. The hashed data is then encrypted, and any non-encrypted fields are merged in to create a full data packet. The full data packet is used to provide a self-authenticating symbol, such as a bar code label, on the self-authenticating document. The self-authenticating code is used during a document verification step to ensure that the document is genuine. The non-encrypted data within the self-authenticating code contains flags indicating which public key should be used to decrypt the encrypted data within the self-authenticating code. After decryption, a checksum is performed and compared against a checksum value stored in the decrypted portion of the self-authenticating code. If they match, and if a digital signature within the self-authenticating code is verified using an appropriate public key, the document is determined to be authentic."

While the self-authentication negotiable document described by Lee et al includes a public key to decrypt data of a self-authenticating document, Applicant submits that Lee et al do not disclose or suggest the creation of an issued certificate that is associated with an establishment of a private key which does not appear on the issued certificate, nor does Lee et al disclose or suggest an authorization which is based upon a submittal at the redemption location of the redemption denomination and the first public key identifier from the issued certificate, a communication of the private key provided by the holder, and a matching comparison of the redemption denomination, the first public key identifier, and the private key stored at said certificate authority.

In contrast to Claim 1 and Claim 16, as amended, Lee includes a "self-authentication" document structure, as seen at least in the Abstract and FIG. 1, which teaches away from the communication of a private key, which does not appear on the issued certificate, as part of the authorization of an issued certificate.

Therefore, Applicant respectfully submits that neither Franklin et al nor Lee et al, alone or combined, disclose or suggest the creation of an issued certificate that is associated with an establishment of a private key which does not appear on

the issued certificate, nor do Franklin et al or Lee et al disclose or suggest an authorization which is based upon a submittal at the redemption location of the redemption denomination and the first public key identifier from the issued certificate, and a communication of the private key provided by the holder, and a matching comparison of the redemption denomination, the first public key identifier, and the private key stored at said certificate authority. As well, it would therefore take significant modification and undue experimentation to meet Claim 1 and Claim 16, as amended.

Therefore, Applicant submits that Claim 1 and Claim 16, as amended, overcome the rejections under 35 U.S.C. §103(a) as being unpatentable over Franklin et al (U.S. Patent No. 6,000,832) in view of Lee et al (U.S. Patent No. 6,170,744 B1). As dependent claims 2-15 depend from amended independent Claim 1, and as dependent claims 17-30 depend from amended independent Claim 16, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

6. Claims 12 and 27 are rejected under 35 U.S.C. §103(a) as being unpatentable over Franklin et al (U.S. Patent No. 6,000,832) in view of Lee et al (U.S. Patent No. 6,000,832) as applied to Claims 11 and 26 respectively, above, and further to Larsson et al (U.S. Patent No. 5,379,344).

The Office Action states that "although Franklin et al do not teach generating a new key for each issued certificate, Larsson et al teach smart card device wherein each new certificate, a new private key is generated. Therefore, it is considered that it would have been obvious to one of ordinary skill in the art at the time of the invention to utilize generating new keys with each new certificate/transaction as this would increase the security of the certificate, making it less likely to forge a certificate".

As described above, Applicant has amended independent Claim 1, to claim a certificate system on a network, comprising:

a certificate authority connected to said network, said certificate authority adapted to allow the definition of a virtual certificate comprising a redemption

denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

a certificate issuance module for creation of an issued certificate upon selectable acquisition of said virtual certificate by an acquirer user across said network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation of said issued certificate associated with a private key which is assigned at time of said acquisition of said virtual certificate, wherein said private key does not appear on said issued certificate, and wherein said redemption denomination, said first public key identifier, and said assigned private key are stored at said certificate authority in association with said issued certificate;

a certificate authentication module for authorization of an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate located at said redemption location, said holder comprising any of said acquirer user and an alternate recipient of said issued certificate to whom said acquirer user has communicated said private key, said authorization based upon a communication from said redemption location to said certificate authority of said redemption denomination and said first public key identifier from said issued certificate, a communication of said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

means to cancel further redemption of said issued certificate at said certificate authority.

Also as described above, Applicant has amended independent Claim 16, to claim a process within a transaction network, comprising the steps of:

defining a virtual certificate on a certificate authority, said defined virtual certificate comprised of a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

creating an issued certificate upon acquisition of said virtual certificate by an acquirer user on said transaction network, said issued certificate comprising

said redemption denomination and said first public key identifier, said creation of said issued certificate associated with an establishment of a private key which does not appear on said issued certificate, said redemption denomination, said first public key identifier, and said established private key stored at said certificate authority in association with said issued certificate;

authorizing an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate, said holder comprising any of said acquirer user and an alternate recipient of said issued certificate to whom said acquirer user has communicated said private key, wherein said authorization is based upon redemption submittal at said redemption location of said redemption denomination and said first public key identifier from said issued certificate, a communication of said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

canceling further redemption of said issued certificate at said certificate authority.

While Larsson et al describe a smart card validation device and method, Applicant respectfully submits that the smart card validation device and method described by Lee et al is significantly different than the present invention, as claimed in Claim 1 and Claim 16, as amended. An overview of the smart card validation device and method, as disclosed by Larsson et al, is seen at least in the Abstract, wherein:

> "A validation device (2) for a smart card (1) of the kind having unprotected data storage memory (4) and protected data storage memory (5) selectively accessible by means of a user access code. The device (2) performs an encryption upon identification data to produce the user access code and reads identification data from the unprotected memory (4) for further encryption. The access code is supplied to the smart card (1) and selected data from said protected memory (5) is read for encryption to produce validating data. A comparator (8) compares the

identification data with the validating data and rejects the smart card (1) if the data do not agree and establishes access to said protected memory (5) if the data do agree."

While the smart card validation device and method described by Larsson et al includes a user access code, Applicant submits that Larsson et al do not disclose or suggest the creation of an issued certificate that is associated with an establishment of a private key which does not appear on the issued certificate, nor does Lee et al disclose or suggest an authorization which is based upon a submittal at the redemption location of the redemption denomination and the first public key identifier from the issued certificate, a communication of the private key provided by the holder, and a matching comparison of the redemption denomination, the first public key identifier, and the private key stored at said certificate authority.

Furthermore, neither Franklin et al, Lee et al, or Larsson et al contain any suggestion, express or implied, that they be combined, to meet Claim 1 and Claim 16, as amended. As well, it would therefore take significant modification and undue experimentation to meet Claim 1 and Claim 16, as amended.

Therefore, Applicant submits that Claim 1 and Claim 16, as amended, overcome the rejections under 35 U.S.C. § 103(a) as being unpatentable over Franklin et al in view of Lee at al, and further in view of Larsson et al. As dependent claim 12 depends from amended independent Claim 1, and as dependent claim 27 depends from amended independent Claim 16, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

8. Applicant has amended dependent Claims 7, 8, 21, 22 and 23, to claim the delivery of the redemption denomination and the first public key identifier to the acquirer user. Support is seen in the Application as filed, at least on page 7, lines 18-20; on page 10, lines 3-6; on page 10, lines 14-20; on page 22, line 31

to page 24, line 11; in Figure 2; in Figure 3; in Figure 4; and in Claims 7, 8, 21, 22 and 23.

Applicant has also amended dependent claims 12 and 27, to claim that the private key is uniquely associated with a single acquired issued certificate. Support is seen in the Application as filed, at least on page 13, line 28; and on page 22, lines 9-10.

CONCLUSION

Applicant therefore respectfully submits that Claims 1-30, as amended, overcome the rejections set forth in the Office Action. Applicant also submits that the amendments do not introduce new matter into the Application. Based on the foregoing, Applicant considers the invention to be in condition for allowance. Applicant earnestly solicits the Examiner's withdrawal of the rejections set forth in the prior Office Action, such that a Notice of Allowance is forwarded to Applicant, and the present application is therefore allowed to issue as a United States patent.

Respectfully Submitted,

Michael A. Glenn
Reg. No. 30,176

Customer No. 22862

Marked-up Version to Show Changes In the Claims

Please amend Claims 1, 7, 8,10, 12, 16, 21-23, 25 and 27 as follows:

1. (Amended Twice) A certificate system on a network, comprising:

a certificate authority connected to said network, said certificate authority adapted to allow the definition of a virtual certificate comprising a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

a certificate issuance module for creation of an issued certificate upon selectable acquisition of said virtual certificate by an acquirer user across said network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation of said issued certificate [comprising] associated with a private key which is assigned at time of said acquisition of said virtual certificate, wherein said private key does not appear on said issued certificate, and wherein said redemption denomination, said first public key identifier, and said assigned private key are stored at said certificate authority in association with said issued certificate;

a certificate authentication module for authorization of an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate located at said redemption location, said holder comprising any of said acquirer user and an alternate recipient of said issued certificate to whom said acquirer user has communicated said private key, said authorization based upon a communication from said [remote] redemption location to said certificate authority of said redemption denomination and said first public key identifier from said issued certificate, [and] a communication of said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

means to cancel further redemption of said issued certificate at said certificate authority.

7. (Amended Twice) The certificate system of Claim 6, wherein said means to deliver said redemption denomination[,] and said first public key identifier[, and said assigned private key] to said acquirer user comprises a printed form of said issued certificate.

8. (Amended Twice) The certificate system of Claim 6, wherein said means to deliver said redemption denomination[,] and said first public key identifier[, and said assigned private key] to said acquirer user comprises an electronic form of said issued certificate.

10. (Amended) The certificate system of Claim 1, wherein said holder of said issued certificate is [an] said alternate recipient who submits said private key.

12. (Amended) The certificate system of Claim 11, wherein said entered, assigned private key is [unique to] uniquely associated with a single acquired issued certificate.

16. (Amended Twice) A process within a transaction network, comprising the steps of:

defining a virtual certificate on a certificate authority, said defined virtual certificate comprised of a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

creating an issued certificate upon acquisition of said virtual certificate by an acquirer user on said transaction network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation of said issued certificate [comprising] associated with an establishment of a private key which does not appear on said issued certificate, said redemption denomination, said first public key identifier, and said established private key stored at said certificate authority in association with said issued certificate;

authorizing an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate, said holder comprising any of said acquirer user and an alternate recipient of said issued certificate to

whom said acquirer user has communicated said private key, wherein said authorization is based upon redemption submittal at said redemption location of said redemption denomination and said first public key identifier from said issued certificate, [and] a communication of said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

canceling further redemption of said issued certificate at said certificate authority.

21. (Amended Twice) The process of Claim 16, wherein said step of creation of said issued certificate comprises a delivery of said redemption denomination[,] and said first public key identifier[, and said established private key] to said acquirer user.

22. (Amended Twice) The process of Claim 21, wherein said delivered redemption denomination[,] and said first public key identifier[, and said established private key to said acquirer user] are included in a printed form of said issued certificate.

23. (Amended Twice) The process of Claim 21, wherein said delivered redemption denomination[,] and said first public key identifier[, and said established private key to said acquirer user] are included in an electronic form of said issued certificate.

25. (Amended) The process of Claim 16, wherein within said authorizing step, said holder of said issued certificate is [an] said alternate recipient [which submits said private key].

27. (Amended) The process of Claim 26, wherein said entered established private key is [unique to] uniquely associated with a single acquired issued certificate.